Department of
INFORMATION
TECHNOLOGY

Maryland Email Security Policy

Last Updated: 05/17/2017

Contents

1.0 Purpose

Employees and contractors of the State may send or receive **confidential information** via email while conducting business. Confidential information and official correspondence must be exchanged securely and protect agency data. The purpose of this policy is to define acceptable guidelines for sending email containing confidential information. The State of Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority.

2.0 Document and Revision History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) sections associated with email security. This document also supersedes any related policy regarding email security declared prior to the 2017 Cybersecurity Program Policy, such as the DoIT Email Encryption Policy and the DoIT Automated E-Mail Forwarding Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Approval of Draft	Maryland CISO
05/17/2017	v1.1	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy applies to all agencies in the Executive Branch of the State of Maryland, employees of those agencies, contractors and vendors supporting those agencies, and any entities or individuals using resources belonging to those agencies — specifically those assigned an email account on a State email system. DoIT will be responsible for ensuring compliance with the policy as outlined in section 4.0 below for Enterprise-managed agencies.

Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy.

4.0 Policy

This policy establishes the appropriate use of a State-issued email account and applies to all personnel, such as: (1) employees, (2) vendors, and (3) agents operating on behalf of a State Executive Branch Agency.

4.1 General Requirements

#	Name	Requirement
A	Compliance with All Policies	All use of email must be consistent with DoIT policies and processes, including but not limited to the *Acceptable Use Policy*.

#	Name	Requirement
		NOTE: Users will be held accountable and responsible for protecting confidential information and for the proper use of public information.
B	Use for Official State Business	All State-issued email accounts should be used primarily for official State purposes; personal communication is permitted on a limited basis as long as it does not interfere with job-related duties and does not lead to the unauthorized distribution of confidential information. Using State-issued email accounts for the purposes of conducting personal business affairs is strictly prohibited (e.g., webhosting, real estate business, or supporting a side business).
C	Employee Type	Email accounts will be labeled with the appropriate employee type that is clearly visible in the email header. Employee types are identified as: ▪ GOVT – Government employee ▪ CONT – Contractor, any non-State employee hired by the State to perform a service ▪ MIL – Military personnel, with an account assigned by the State, such Air National Guard
D	Confidential Information Security	Data loss prevention (DLP) solutions, where available, should filter all email traffic for confidential information.
E	Electronic Communication Ownership	Messages created, sent, and received on a State-issued email are property of the State of Maryland.
F	Monitoring	Messages created, sent, and received through State-issued email may be monitored without prior notice.
G	Attachment Security	Filters will be used to prevent the receipt of unauthorized attachments.
H	Training	Users must be trained on email security precautions annually. These records will be maintained in accordance with the *Acceptable Use Policy*.

4.2 Automatic Email Forwarding

The State has established controls to ensure that email is retained and stored within the United States, is encrypted while at rest, and is recoverable for historical analysis.

Employees and contractors for the State may receive confidential information to their Maryland.gov email addresses and may also conduct official business for the benefit of the State using their Maryland.gov email addresses. However, no automated exchange of confidential information or official correspondences is permitted; all official email correspondence and all email containing confidential information must be explicitly user-generated and provide the State with the ability to maintain a record of such exchanges.

#	Name	Requirement
A	Automated Forwarding from Maryland.gov	▪ Automated email forwarding features will be eliminated from the Maryland.gov email domain ▪ Exception will only be granted on a case-by-case basis with the written approval of: ◆ State CISO or delegated authority (if IT is managed by DoIT)

#	Name	Requirement
		- Deputy CIO or delegated authority (if under policy authority but not actively managed by DoIT)
B	Forwarding of Individual Messages	Nothing in this policy bans a user from explicitly sending email to an external email account provided appropriate precautions are taken to protect confidential information.
C	Filters Allowed	Filters may be used to automatically forward messages under this policy if confidential information is not contained in the messages.
D	Automated Forwarding to Maryland.gov	Users are permitted to automatically forward their external mail to a Maryland.gov email address. NOTE: All messages received at the Maryland.gov email domain become the property of the State of Maryland.

4.3 Email Encryption

Any employee who uses email to send confidential information shall use an appropriate encryption service. Email encryption and other security requirements concerning confidential information are outlined in the table below.

#	Name	Requirement
A	Encryption to External Recipients	Employees and contractors shall utilize encryption if they have a business need that requires sending confidential data by email to an external email address. ▪ Employees and contractors utilizing the Maryland.gov email system may obtain an encryption license provided by DoIT ▪ Agencies using non-DoIT-supported email systems must independently procure a solution to encrypt email sent to external addresses
B	Subject Line	Employees and contractors shall not place confidential information in the “Subject” line of any email message whether to internal, State-associated personnel, or to external recipients.
C	Subject Line to External Recipients	Employees and contractors who receive confidential information — within an email or in the subject line — from an external sender shall not reply to the message unless they utilize encryption and remove the confidential information from the reply message and subject line.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency’s mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Acceptable Use Policy

- Data Security Policy
- Public and Confidential Information Policy
- Remote Access Policy

7.0 Definitions

Term	Definition
Confidential Information	Confidential information is non-public information that, if disclosed, could result in a negative impact to the State of Maryland, its employees, or citizens and includes the following sub-categories: ▪ Personally Identifiable Information ▪ Privileged Information ▪ Sensitive Information For more information on confidential information see *Confidential Information Policy*.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for enforcing email security for onboarded Enterprise agencies. DoIT will enforce email security per established minimum requirements as outlined in section 4.0 unless an agency has completed a Policy Exemption Request Form and received approval from DoIT. Agencies under the policy authority of DoIT, but not under direct management, must enforce email security to meet the requirements established in section 4.0.

If DoIT determines that an agency is not compliant with the *Email Security Policy*, the agency will be given sixty (60) days to become compliant per the requirements in this policy. After such time, if the agency remains out of compliance the Secretary of Information Technology will be notified and remediation will be mandated.

Any attempt to circumvent email security safeguards (e.g., intentionally sending confidential information to external personnel without using proper encryption) will be considered a security violation and subject to investigation and potential disciplinary action, which may include written notice, suspension, termination, and possible criminal and/or civil penalties.